Jennifer Lynch (SBN 240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Jason M. Schultz (SBN 212600)
jschultz@law.berkeley.edu
Lila I. Bailey (SBN 238918)
lbailey@law.berkeley.edu
Aaron Mackey (Application for Student Practice Pending)
Jose de Wit (Application for Student Practice Pending)
SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
U.C. Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-1957
Facsimile: (510) 643-4625

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ELECTRONIC FRONTIER FOUNDATION,

Plaintiff,

v.

DEPARTMENT OF DEFENSE, *et al.*,

Defendants.

Case No. 09-cv-05640-SI

NOTICE OF CROSS MOTION FOR SUMMARY JUDGMENT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF CROSS MOTION FOR SUMMARY JUDGMENT

AND

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Date: Friday, Jan. 13, 2012
Time: 9:00 a.m.
Place: Courtroom 10, 19th Floor
Judge: Hon. Susan Illston

NOTICE OF MOTION

TO DEFENDANTS AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on January 13, 2012, or as soon thereafter as the matter may be heard in Courtroom 10 on the 19th floor of the United States District Court for the Northern District of California, 450 Golden Gate Ave., San Francisco, California, Plaintiff Electronic Frontier Foundation ("EFF") will, and hereby does, cross move for summary judgment.

Pursuant to Federal Rule of Civil Procedure 56, Plaintiff seeks an order requiring the Department of Justice and its components the Federal Bureau of Investigation ("FBI") and Criminal Division ("DOJ"), and the Department of Homeland Security ("DHS") and its components the Immigration and Customs Enforcement ("ICE") and the Secret Service to release records improperly withheld from the public under the Freedom of Information Act ("FOIA"). Plaintiff respectfully asks that this Court issue an order requiring DOJ, FBI, DHS, ICE, and the Secret Service to release records improperly withheld from the public. This cross motion is based on this notice of cross motion, the memorandum of points and authorities in support of this cross motion, the declaration of Jennifer Lynch and attached exhibits in support of this cross motion, and all papers and records on file with the Clerk or which may be submitted prior to or at the time of the hearing, and any further evidence which may be offered.

DATED: November 17, 2011

Respectfully submitted,

By: /s/ Jason M. Schultz

Jason M. Schultz
jschultz@law.berkeley.edu
Lila I. Bailey
SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
U.C. Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-1957
Facsimile: (510) 643-4625

Jennifer Lynch
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION

454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statute

Federal Rule

Federal Regulations

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff Electronic Frontier Foundation (EFF) filed this action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, seeking records about how government agencies use online social networks to collect information on Americans' use of digital networks, investigate crime, and surveil, monitor, and track the public. Lynch Decl. ¶ 6, Ex. 1. Such information is vital to the ongoing public debate about the impact such activities have on our privacy and civil liberties, and EFF, which for 21 years has defended civil liberties in new technologies, has a proven track record of obtaining similar information from the government and disseminating it to the public. *See* Electronic Frontier Foundation, FOIA, http://www.eff.org/issues/foia (last visited Nov. 16, 2011).

In the past several years, the news media has increasingly reported on law enforcement agencies' use of social networks in their investigations. Lynch Decl. ¶ 7, Ex. 2. Yet the government itself has provided very little information about these activities or the standards it follows to protect Americans' civil liberties and privacy interests. With over 800 million active users on the popular social networking site Facebook alone, *id*. at ¶ 8, Ex. 3, this raises important questions about how the government conducts these activities and what safeguards and oversight mechanisms are in place to protect us from violations of our rights.

To find answers to these questions, EFF sent FOIA requests to various federal law enforcement agencies in October 2009 seeking copies of agency guidelines, manuals, and procedures discussing how the various agencies use social networking websites in investigations and to gather data. *Id*. at ¶ 6, Ex. 1. When the agencies failed to respond to EFF's requests, EFF filed suit.

As a result of this lawsuit, the agencies have collectively disclosed several hundred pages, which have provided meaningful insight into, for example, the U.S. Citizenship and Immigration Services' patrolling of social media, the manuals created by social networking websites to handle law enforcement requests for user information, and information on DHS' use of Twitter and other

social networks to monitor individuals online. Lynch Decl. ¶¶ 4-5. However, the agencies have withheld several hundred more pages in part or in full and continue to assert, improperly, that these records can be withheld pursuant to FOIA Exemptions 4, 5, and 7(E).[1] In several cases, the agencies have also failed to sufficiently justify their withholding of information and properly segregate non-exempt material. Finally, Defendant Immigration and Customs Enforcement has not conducted an adequate search for responsive records. For the reasons set forth below, EFF opposes Defendants' Motion and cross-moves for summary judgment. Plaintiff respectfully requests that the Court deny Defendants' Motion, grant its Cross Motion and order Defendants to process and disclose the withheld records immediately.

II. FACTUAL BACKGROUND

EFF does not dispute Defendants' statement of facts, save for the challenges that Plaintiff outlined in the Introduction above and presents more fully in the Argument below. Since filing its complaint, EFF has greatly narrowed the remaining issues with the Defendants.[2] EFF now cross moves for Summary Judgment on the remaining claims against the remaining Defendants—the Department of Justice, Criminal Division ("DOJ"), the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), and the Secret Service.

III. STANDARD OF REVIEW

The Freedom of Information Act is intended to safeguard the American public's right to know "what their Government is up to." *DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989). The central purpose of the statute is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). "[D]isclosure, not secrecy, is the dominant objective of the [FOIA]." *Dep't of Air Force v.*

[1] EFF does not challenge information withheld under Exemptions 1, 2, 6, 7(C) and 7(D). Lynch Decl. ¶ 9.

[2] Plaintiff dismissed seven parties and has agreed not to challenge four exemptions. Lynch Decl. ¶¶ 9-10.

Rose, 425 U.S. 352, 361 (1976). The Supreme Court has stated that "[o]fficial information that sheds light on an agency's performance of its statutory duties falls squarely within [the] statutory purpose." *Reporters Comm.*, 489 U.S. at 773.

Unless "the requested material falls within one of . . . nine statutory exemptions, the FOIA requires that records and material in the possession of federal agencies be made available on demand to any member of the general public." *Robbins Tire,* 437 U.S. at 221; *Nat'l Wildlife Fed'n v. U.S. Forest Service*, 861 F.2d 1114, 1116 (9th Cir. 1988). The exemptions "have been consistently given a narrow compass," and agency records that "do not fall within one of the exemptions are improperly withheld[.]" *DOJ v. Tax Analysts*, 492 U.S. 136, 151 (1989) (internal quotation marks omitted). Further, agencies cannot use the FOIA's exemptions to withhold agency "secret law," which runs counter to the FOIA's purpose. *See NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 153 (1975).

FOIA disputes involving the propriety of agency withholdings are commonly resolved on summary judgment. *Nat'l Wildlife Fed'n*, 861 F.2d at 1114. Summary judgment is proper when no genuine and disputed issues of material fact remain and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Feshbach v. SEC*, 5 F. Supp. 2d 774, 779 (N.D. Cal. 1997) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986)). A moving party who bears the burden of proof on an issue at trial "must affirmatively demonstrate that no reasonable trier of fact could find other than for the moving party." *Id*. "In contrast, a moving party who will not have the burden of proof on an issue at trial can prevail merely by pointing out that there is an absence of evidence to support the nonmoving party's case." *Id*.

A court reviews the government's withholding of agency records *de novo*, and the government bears the burden of proving that a particular document falls within one of the nine narrow exemptions to the FOIA's broad presumption of disclosure. 5 U.S.C. § 552(a)(4)(B); *Reporters Comm.*, 489 U.S. at 755. An agency must prove that "each document that falls within the class requested either has been produced, is unidentifiable, or is wholly exempt from the Act's inspection requirements." *Goland v. CIA*, 607 F.2d 339, 352 (D.C. Cir. 1978) (internal citation and

quotation omitted). When claiming one of the FOIA's exemptions, the agency bears the burden of providing a "'relatively detailed justification' for assertion of an exemption, and must demonstrate to a reviewing court that records are clearly exempt." *Birch v. U.S. Postal Service*, 803 F.2d 1206, 1209 (D.C. Cir. 1986) (citing *Mead Data Cent., Inc. v. Dep't of the Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977)). An agency may submit affidavits to satisfy its burden, but "the government may not rely upon conclusory and generalized allegations of exemptions." *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir. 1995) (quoting *Church of Scientology v. Dep't of Army*, 611 F.2d 738, 742 (9th Cir. 1980) (internal quotation marks omitted)).

IV. ARGUMENT

As described in detail below, Defendants have failed to release all non-exempt materials in response to Plaintiff's FOIA requests. Specifically, they have improperly asserted FOIA Exemptions 7(E), 5, and 4. Defendants have also insufficiently justified their withholdings and failed to segregate non-exempt material, while ICE has conducted an inadequate search for responsive records. As a result, the Court should deny the government's motion for summary judgment, grant Plaintiff's cross motion for summary judgment, and order Defendants to release all improperly withheld material.[3]

A. Defendants Have Improperly Withheld Agency Records Under Exemptions 7(E), 5, and 4.

1. Defendants Have Improperly Withheld Publicly Known and Routine Law Enforcement Techniques, Boilerplate Search Warrant Affidavits and "Areas of Focus," and So-Called "Secret Law" Policy Statements Under Exemption 7(E) Without Demonstrating the Requisite Risk of Circumvention.

Exemption 7(E) allows the government to withhold documents only if it demonstrates a reasonable risk that criminals will use them to circumvent detection, apprehension or prosecution. *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1035 (N.D. Cal. 2005). Here, however, Defendants have improperly withheld three categories of documents that fail to meet this standard.[4] First,

[3] EFF has listed the improperly withheld records it is challenging below in the beginning footnotes under the relevant section that addresses each improperly asserted exemption.

[4] Plaintiff challenges the withholding or redaction of material under Exemption 7(E) in the following documents: DOJ Items 3-4, 8-13; DHS/ICE Docs. 1-5, 33; Secret Service Docs. 1-21;

Defendants have withheld records that describe publicly known and routine law enforcement techniques; disclosing these techniques cannot create a circumvention risk because criminals already know of them or could easily surmise what they are. Second, the DOJ has withheld boilerplate search warrant affidavits, and the FBI has withheld information about its "areas of focus" from nearly every record responsive to this FOIA request, based on nothing more than mere speculation concerning risk of circumvention. Third, the DOJ and the FBI have withheld guidelines, policy documents, and legal standards that establish so-called "secret law"—rules for whether and how the agencies may take action affecting the public; withholding these is impermissible for public policy reasons discussed further below in Section IV.A.1.c.

Exemption 7(E) exempts from disclosure "records or information compiled for law enforcement purposes" that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). To claim an exemption under 5 U.S.C. § 552(b)(7)(E), the government must show that (1) the records were compiled for law enforcement purposes and that (2) the records reveal techniques, procedures or guidelines for law enforcement investigations that, if disclosed, could reasonably be expected to risk circumvention of law. *Gordon*, 388 F. Supp. 2d at 1035.

To meet this burden, Defendants must support their circumvention claims with specific descriptions of the withheld information and "substantial evidence" or credible testimony. *See Feshbach*, 5 F. Supp. 2d at 786; *Gerstein v. DOJ*, No. C-03-04893 RMW, 2005 U.S. Dist. LEXIS 41276, at *41 (N.D. Cal. Sept. 30, 2005) (rejecting government's circumvention claim because risk was remote and unsupported by evidence or expert affidavits). Moreover, Exemption 7(E) does not protect law enforcement techniques and procedures that are generally known or would leap to the mind of a "simpleminded investigator." *Rosenfeld v. DOJ*, 57 F.3d 803, 815 (9th Cir. 1995);

---

and all FBI information withheld under 7(E), except for Bates 10-12, 25-28, portions of Bates No. 123-25 that discuss "limitations when investigating a particular social networking site," and any redactions of email addresses or internal web addresses.

Albuquerque Publ'g Co. v. DOJ, 726 F. Supp. 851, 857-58 (D.D.C. 1989); *Hamilton v. Weise*, No. 95-1161-CIV-ORL-22, 1997 U.S. Dist. LEXIS 18900, at *30-32 (M.D. Fla. Oct. 1, 1997). Nor does it protect policies or legal standards that regulate an agency's dealings with members of the public. *Gordon*, 388 F. Supp. 2d at 1036-37.

a. Defendants Have Improperly Withheld Law Enforcement Techniques That Are Generally Known or Routine.

Defendants have improperly withheld numerous records under Exemption 7(E) that describe law enforcement techniques or procedures that are routine or well-known to the public, nevertheless claiming that they should somehow remain secret. *See, e.g.*, Ulmer Decl. ¶¶ 64-65 (claiming that disclosing a Secret Service technique or releasing any information about it "could nullify the future effectiveness of these protective and investigative measures"); Hardy Decl. ¶¶ 61-63 (claiming that describing FBI's online investigative techniques or procedures "could jeopardize ongoing criminal investigations and any future criminal investigations").

Yet despite such sweeping statements, Defendants cannot withhold information about techniques or procedures that are routine or already widely known. *See Albuquerque Publ'g Co.*, 726 F. Supp. at 857-58 (directing agencies to release records "pertaining to techniques that are commonly described or depicted in movies, popular novels, stories or magazines, or on television," including eavesdropping, wiretapping, and surreptitious tape recording and photographing); *Hamilton*, 1997 U.S. Dist. LEXIS 18900, at *30-32 (holding that generally known techniques include those discussed in judicial opinions); *Rosenfeld v. DOJ*, 761 F. Supp. 1440, 1450 (N.D. Cal. 1991) (holding that details about a pretextual phone call were not protected because the technique would "leap to the mind of the most simpleminded investigator"). Because the public—including criminals—already know about these techniques, disclosing records that discuss them will not create a circumvention risk.

In this case, Defendants have improperly withheld documents that discuss both well-known and routine law enforcement techniques. First, law enforcement techniques involving social networks are already widely known, having been depicted in mass media and described in judicial opinions. Some examples of these include:

- **Monitoring social networking websites for potential and actual criminal activity:** Many of the techniques Defendants use to monitor social networks for criminal activity turn up with a Google search, including a document Defendant DOJ has withheld in this very case. This document, entitled "How to Effectively Search MySpace.com: A Guide for Investigators," Ellis Decl. ¶ 26, DOJ Item 12, is publicly available online. Lynch Decl. ¶ 11, Ex. 5. This directly calls into question the accuracy of Defendants' 7(E) withholdings and their assessment of the documents at issue. Further, records Defendants have already released in this case and numerous news articles describe how law enforcement agencies regularly monitor social networking sites to identify criminal activity before it develops. DHS/ICE Doc. 8; Lynch Decl. ¶ 12, Ex. 6; *id.* at ¶ 13, Ex. 7 (attaching news articles describing efforts by local and federal police to use social networking websites in their investigations). In fact, the public's knowledge that law enforcement agencies use social networks to monitor criminal activity is so pervasive that such efforts have literally become the punch line of parodies. *See CIA's 'Facebook' Program Dramatically Cuts Agency's Costs*, The Onion News Network (last visited Oct. 29, 2011); Lynch Decl. ¶ 14, Ex. 8 (video clip satirically depicting Facebook as "the massive online surveillance program run by the CIA" to monitor people and describing friend requests as a method for "infiltrating the networks of suspected dissidents").

- **Creating fake profiles and using pretext to observe criminal activity:** People often lie about their age and other personal details on social networks, so it is no surprise that police do the same when investigating crime online. Lynch Decl. ¶ 15, Ex. 9. Using pretext to discover evidence of criminal activity is a timeless technique. *See Rosenfeld*, 57 F.3d at 815 (describing use of a pretextual phone call during an FBI investigation). Examples of police using deception online are numerous. In one high-profile incident, police posed as an attractive college-aged woman on Facebook, sending friend requests to college students to gain access to evidence of underage drinking saved in their private profiles. *See* Simma Aujla, *Police Officers Set Up Facebook Account to Catch Underage Drinkers*, The Chronicle of Higher Education (Dec. 8, 2009); Lynch Decl. ¶ 16, Ex. 10; *see also id.* at ¶ 17, Ex. 11 (attaching additional news articles

about law enforcement's use of pretext in investigations). Further, agency records released in this FOIA case document how the same technique has been used to ensnare tax cheats, *id*. at ¶ 18, Ex. 12, determine whether individuals are actually married for purposes of securing legal residency in the United States, *id*. at ¶ 19, Ex. 13, and to generally monitor criminal activity. DHS/ICE Doc. 8. Police also use pretext in child exploitation investigations. *See U.S. v. Patten*, 397 F.3d 1100, 1101 (8th Cir. 2005) (describing law enforcement's use of pretext in a chat room to investigate and lure a suspected child predator). On television, NBC has even devoted an entire national primetime series, "To Catch a Predator," to this technique. Lynch Decl. ¶ 20, Ex. 14.

- **Using location information contained in social networking sites to track an individual's movement:** On social networks, people can be tracked down—literally. The websites allow individuals to explicitly mention their location or use location-based tags, which police can easily use to track and apprehend suspects. In one case, police arrested a theft suspect after the individual posted on Twitter where he was celebrating his birthday. *See* Alice Lipowicz, *For law enforcement, social media can cut both ways*, Government Computing News (April 8, 2011); Lynch Decl. ¶ 21, Ex. 15. This technique has been used in other law enforcement investigations. *Id*. at ¶ 22, Ex. 16. Additionally, several software programs exist that allow anyone, be it police or a private citizen, to download location information about a particular social network user and compile a map of his or her past and present locations. Lynch Decl. ¶ 23, Ex. 17 (describing a geolocation aggregation program known as "Creepy").

- **Using social networks to monitor gang activity:** The public also knows that law enforcement uses social networks to investigate gangs. An article reporting on a national law enforcement conference describes how "[g]ang members have been captured after posting photographs of themselves on Facebook or Twitter displaying tattoos and inscribed gang necklaces. Some of the suspects pose on Facebook with stolen money or guns, or show videos of themselves on YouTube with cars that have been identified as evidence in a crime." *Id*. at ¶ 21, Ex. 15.

- **Using social networking websites to compile personal information about individuals:** Social networks provide enormous amounts of personal information for law enforcement to mine. A recent news article reports on how the CIA compiles information from social networking websites such as Twitter to collect intelligence and predict future behavior. *See* Kimberly Dozier, *AP Exclusive: CIA Tracks revolt by Tweet, Facebook*, The Associated Press (Nov. 4, 2011); Lynch Decl. ¶ 24, Ex. 18. Indeed, documents previously released in this case describe the CIA's program, which is known as the "Open Source Center." *Id*. at ¶ 25, Ex. 19. Similarly, the FBI has taken interest in a project developed at the University of Arizona called the "Dark Web Project" that purports to predict future terrorist behavior. FBI Bates Nos. 1-4; Lynch Decl. ¶ 26, Ex. 20. These data-crunching techniques are no longer used by law enforcement alone; in recent months, private online activists have used similar tactics to build profiles of individuals they are targeting for social or political reasons. *See* Peter Bright, *Dox everywhere: LulzSec under attack from hackers, law enforcement*, Ars Technica (last visited Nov. 15, 2011); Lynch Decl. ¶ 27, Ex. 21.

- **Using software to track a user's entire computer or network activity:** Technology also allows law enforcement to track people's digital movements online using software. Often known as a "sniffer," the programs can monitor a user's entire activity on a particular computer or network, including all websites the user has visited and the content he or she has downloaded. *See* Lynch Decl. ¶ 28, Ex. 22 (news article describing the technology). The technique is widely used in law enforcement; police have used it in sting operations and courts have used it to monitor parolees. *See, e.g.*, *U.S. v. Gorkshov*, No. 00-550C, 2001 WL 1024026, *1 (W.D. Wash. May 23, 2001) (describing the FBI's use of a "sniffer" to track and store information about defendant's conduct during a sting operation, including defendant's username and password to another computer network); *U.S. v. Lifshitz*, 369 F.3d 173, 177 n.3 (2nd Cir. 2004) (describing a court-imposed parole restriction requiring defendant to install "systems that enable the probation officer or designee to monitor and filter computer use").

In light of the vast amount of public knowledge about online law enforcement techniques, Defendants bear a high burden under Exemption 7(E) to show that the materials they have withheld contain specific techniques that are *not* generally known to the public. *Albuquerque Publ'g Co.*, 726 F. Supp. at 858. This information plainly contradicts Defendants' broad, unsupported claims that their use of online investigative techniques is not generally known. *See, e.g.*, Def's Brf. at 17, 19, 20; Ulmer Decl. ¶ 65; Hardy Decl. ¶ 63; Holzer Decl., Ex. 1 Docs. 1-5.

To provide but one example, ICE has redacted under 7(E) all information other than headings and its own seal from a 25-page presentation entitled "Internet Exploitation for Gang Investigations," DHS/ICE Doc. 2, even though law enforcement's investigation of gang activity online has been well-documented in the media. Lynch Decl. ¶ 21, Ex. 15. Defendants have also withheld information about many other widely known law enforcement techniques. *See, e.g.*, DHS/ICE Doc. 5 (presentation on using Internet for investigations); Secret Service Doc. 8 (search terms used to detect threats against Secret Service protectees); DOJ Items 8-13 (training materials for using social networking sites to investigate crimes); Hardy Decl. pp. 133, 138, 141, 157 (same). Even from the vague descriptions in Defendants' Vaughn indices and affidavits, it is clear that much of the information they have withheld describes well-known procedures and techniques. Disclosing well-known law enforcement methods cannot create a circumvention risk; therefore Defendants must release information about any technique, procedure or guideline that is not secret. *Gordon*, 388 F. Supp. 2d at 1035.

Similarly, routine techniques, such as using pretext to obtain information, eavesdropping, and wiretapping, do not become unique and subject to Exemption 7(E) protections merely because they occur online or in the context of social media. Nevertheless, Defendants have withheld records that describe routine law enforcement techniques without explaining why a technique that is routine or well-known offline is any less routine or less well-known when applied online. For example, the FBI argues that, although some of the techniques it has withheld are routine or well-known, they nevertheless remain secret when used online. Hardy Decl. ¶¶ 61-63.

Criminals who are aware of offline techniques would likely assume that the same techniques are being used on the Internet. For example, courts have recognized that law enforcement agents can gain access to one's physical mail, email, or voicemail as part of an investigation. *Warshak v. U.S.*, 532 F.3d 521, 524 (6th Cir. 2008) (describing law enforcement technique for gaining access to suspects' email); *Dunaway v. Webster*, 519 F. Supp. 1059, 1082-83 (C.D. Cal. 1981) (describing law enforcement technique for gaining access to suspects' physical mail as "routine"). Given that email has been in use for 23 years, Dave Crocker, "Email History," The World's First Web Published Book; Lynch Decl. ¶ 29, Ex. 23, and 800 million people use Facebook, *id*. at ¶ 8, Ex. 3, it is no less obvious that law enforcement would attempt to gain access to one's email or private messages on sites like Facebook. The fact that such messages are "electronic" makes the technique no less routine or generally known. The same is true for eavesdropping on a suspect's workplace, school, or personal conversations or using subterfuge to join a suspect group, *id*. at ¶ 30, Ex. 24; similar techniques would be used to eavesdrop on chat rooms or surreptitiously infiltrate a suspect's online "friend" group. Because the online equivalents of these techniques are just as well-known and routine as their offline counterparts, Defendants must release any records that describe them.

b. DOJ and FBI Cannot Withhold Search Warrant Affidavit Templates or "Areas of Focus" Because They Have Failed To Demonstrate Any Circumvention Risk From Disclosing Them.

In addition to generally known and routine techniques, the DOJ and the FBI are withholding search warrant affidavit templates and documents concerning "areas of focus" without any evidence that their release poses a reasonable risk of circumvention.

The DOJ has withheld two search warrant affidavit templates for searching the social networking websites MySpace and Facebook, arguing that releasing the documents would give criminals a blueprint to circumventing the law. Ellis Decl. ¶ 26, DOJ Items 3-4. This argument fails for two reasons. First, numerous search warrants and supporting affidavits involving online social networks are publicly available for download from district court websites through PACER. Lynch Decl. ¶ 31, Ex. 25. The DOJ also makes search warrant affidavit templates available among its

online resources for law enforcement investigators. *Id*. at ¶ 32, Ex. 26. Thus, any theoretical risk that might occur from disclosing the search warrant affidavit templates has almost certainly already occurred from the disclosure of both the actual warrant affidavits in the public record and the templates the DOJ has voluntarily made available. In short, any "blueprint" that the agency is concerned criminals might discover can already be found in court records and on the DOJ's own website. At a minimum, the DOJ must demonstrate what *additional* risks would occur from disclosing the withheld affidavits over what is already publicly available.

Second, the Ninth Circuit and many other jurisdictions recognize a First Amendment or common law presumptive right of access to search warrants and their related documents once a warrant is executed or an indictment is issued. *See, e.g.*, *U.S. v. Bus. of the Custer Battlefield Museum and Store Located at Interstate 90, Exit 514, So. of Billings, Montana*, 658 F.3d 1188, 1196-97 (9th Cir. 2011). Thus, if the information contained in the DOJ's templates has not already been disclosed, it will almost certainly be so soon.

The FBI has also improperly withheld records under 7(E) concerning its "areas of focus," asserting only broad, speculative, and unsupported claims that disclosure would risk circumvention of the law.[5] These documents contain the names of Internet sites where the FBI conducts investigations; the titles of divisions, units or teams engaged in online investigations; the geographic location of divisions participating in online investigations; and other information described broadly as techniques and procedures that would reveal the "potential online focus of law enforcement investigations."[6] However, the FBI presents no evidence or qualified testimony to support its argument that disclosure could lead to circumvention. Hardy Decl. ¶¶ 62-64 ("[p]ublic disclosure of this information could allow circumvention of the law by indicating which cyber venues are safer for illegal activity[]"). Under this District's precedent, such records must be

[5] The FBI's declaration specifically asserts this theory to justify particular redactions to every document withheld under 7(E) except for Bates Nos. 5-9, 10-12, 25-28, 55-56 and 123-25. Hardy Decl., Ex. I. *See also* Hardy Decl. pp. 35-37, 41-43, 73 and 133. The FBI also generally advances this argument for all of its withholdings under 7(E). *See* Hardy Decl. ¶¶ 62-63.

[6] For instance, FBI asserts 7(E) to "protect the descriptive titles of certain divisions, units, or teams whose existence and function, if known, may serve to warn those involved in cyber crime where the FBI is concentrating its criminal investigation or law enforcement efforts." Hardy Decl. ¶ 62.

released unless the government presents evidence or expert testimony showing that criminals are actually likely to use the information to thwart law enforcement efforts. *See Gerstein v. DOJ*, No. C-03-04893 RMW, 2005 U.S. Dist. LEXIS 41276, at *41 (N.D. Cal. Sept. 30, 2005). In *Gerstein*, Judge Whyte of the Northern District of California rejected an argument that is nearly identical to the FBI's argument here. There, the DOJ argued that it could not release information about particular U.S. attorneys' use of PATRIOT Act delayed-notice warrants, claiming that it would allow wrongdoers to focus their efforts on "soft" jurisdictions." *Id*. at *39. Judge Whyte rejected this argument, holding that conclusory testimony that "criminals could capitalize on knowing which jurisdictions have yet to use [the warrants]" did not satisfy that burden because the affiant, a DOJ attorney, was untrained in criminal psychology or criminology and cited no evidence to support the theory. *Id.* at *41. Here, the FBI's affiant, a FOIA official, has failed to attest to training in either criminal psychology or criminology, Hardy Decl. ¶ 1-3, and has failed to present evidence that a circumvention risk exists. Yet Mr. Hardy advances the same conclusory claim that "[p]ublic disclosure of this information could allow circumvention of the law by indicating which cyber venues are safer for illegal activity[]" as the affiant in *Gerstein*. *Compare id. at* ¶ 63 to *Gerstein*, 2005 U.S. Dist. LEXIS 41276, at *41.

Moreover, the FBI's argument here fails for the same logical reasons the Court rejected it in *Gerstein*. First, the court recognized that a particular jurisdiction's use of delayed-notice warrants in the past did not reliably predict whether it would use them in the future. 2005 U.S. Dist. LEXIS 41276, at *40-41. Second, the court reasoned that the general notion that certain jurisdictions are "softer" than others did not give criminals specific enough information to tailor their illegal activities accordingly. *Id*. Here, the FBI does not explain how information about its "areas of focus" over the past four years is any more reliable in helping criminals predict the agency's future enforcement activities. Hardy Decl. ¶¶ 61-63. Further, the general notion that the FBI has concentrated its efforts on certain locations, websites, or "areas of focus" does not tell criminals how they can specifically change their behavior to circumvent the law. *See Gerstein*, 2005 U.S. Dist. LEXIS 41276, at *40-41. Because *Gerstein* rules out such unsupported, broad and speculative

claims as the basis for withholding material under Exemption 7(E), the FBI must disclose all information withheld under this theory.

c. DOJ and FBI Have Improperly Withheld Guidelines and Policies that Regulate an Agency's Dealings With the Public.

Finally, the DOJ and the FBI have inappropriately withheld guidelines, policy documents, and legal standards under Exemption 7(E) that establish rules for whether and how the agencies may take action affecting the public. Courts have repeatedly rejected attempts to withhold policies and standards such as these. *See NLRB v. Sears, Roebuck & Co.,* 421 U.S. 132, 153 (1975) (holding that Exemption 7(E) does not protect statements of agency policy or other documents that have the "force and effect of law"); *Jordan v. DOJ,* 591 F.2d 753, 781 (D.C. Cir. 1978) (en banc) (recognizing that one of the fundamental purposes of the FOIA is to ensure that agencies do not maintain a secret body of law that regulates their dealings with the public); *Gordon*, 388 F. Supp. 2d at 1028 (holding 7(E) inapplicable to documents describing the legal basis for detaining someone on the FBI's "no-fly" watch list).

In applying this rule, the *Gordon* case is instructive. There, the FBI withheld records describing the legal basis for detaining someone whose name appeared on the FBI's "no-fly list" and other terrorist watch lists, which the agency claimed would help criminals circumvent the law. *Gordon*, 388 F. Supp. 2d at 1036-37. The Court rejected this argument because the agency failed to show that releasing the records, which described a legal standard that regulated the agency's dealings with members of the public, would risk circumvention of the law. *Id*. Similarly, in *PHE, Inc. v. DOJ*, the court rejected a similar DOJ argument about a "step by step analysis" and prosecutorial guidelines concerning obscenity crimes, explaining that such standards are "precisely the type of information for release under FOIA." 983 F.2d 248, 252-43 (D.C. Cir. 1993).

Here, the DOJ and the FBI have withheld records that have the "force and effect of law" and must be disclosed. *See* DOJ Items 3-4 (search warrant affidavit templates); FBI Bates Nos. 42-54 (guidelines for use of undisclosed investigative technique), 76-77 (standards for requesting user information from online service), 79-80 (guidelines for use of online services in investigations). The documents are analogous to those withheld in *Gordon*, in that they either describe the general

legal standards for when to conduct a search on social networks or regulate other aspects of the Defendants' dealings with the public. As such, the documents must be released.

2. ICE, FBI, and Secret Service Have Also Improperly Withheld Records Under the Exemption 5 Attorney-Client, Attorney Work Product, and Deliberative Process Privileges.

ICE, the FBI and the Secret Service have not met their burden to withhold records under Exemption 5 because they have failed to show that the attorney-client, deliberative process, or work product privileges apply to the withheld documents.[7] In addition, Defendants improperly use the exemption to shield agency "working law" from the public.

FOIA contains a narrow exemption for "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency[.]" 5 U.S.C. § 552(b)(5). Exemption 5 protects a record from disclosure where "its source [is] a government agency," and where the withheld material falls "within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it." *Dep't of the Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001).

However, Exemption 5 does not allow agencies to withhold documents that "constitute the 'working law' of the agency." *Sears*, 421 U.S. at 153. "Exemption 5, properly construed, calls for disclosure of all opinions and interpretations which embody the agency's effective law and policy including final opinions, statements of policy and interpretations which have been adopted by the agency, and instructions to staff that affect a member of the public." *Id*. (citing 5 U.S.C. § 552(a)(2)) (internal quotations omitted). Such documents "are not the ideas and theories which go into the making of the law, they are the law itself, and as such should be made available to the public." *Niemeier v. Watergate Spec. Prosecution Force*, 565 F.2d 967, 974 (7th Cir. 1977).

Defendants have improperly claimed three privileges under Exemption 5 to shield information from disclosure in this case: the attorney-client privilege, the attorney work product privilege, and the deliberative process privilege.

[7] Plaintiff challenges the following documents improperly withheld under Exemption 5: DHS/ICE Doc. 3; Secret Service Doc. 11; FBI Bates Nos. 10-12, 25-28, 40-41, 55-56, 57-59, 63-64, 69-70, 76-77, 78-80, 84-87, 88-94, 96, 126-29, and 150-56.

a. ICE and FBI Have Improperly Withheld Under Exemption 5 Records That Are Not Subject to the Attorney-Client Privilege.

ICE and the FBI assert Exemption 5's attorney-client privilege to impermissibly shield agency policy and working law. The privilege protects confidential communications by a specific client to a specific attorney to obtain legal advice for a specific set of circumstances, *Fischer v. U.S.*, 425 U.S. 391, 403 (1976), and opinions from the attorney to the client based on those specific facts. *Feshbach*, 5 F. Supp. 2d at 784 (N.D. Cal. 1997) (citing *Brinton v. Dep't of State*, 636 F.2d 600, 603 (D.C. Cir. 1980)). However, the privilege is narrowly construed, protecting "only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege." *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 862 (D.C. Cir. 1980) (citing *Fischer*, 425 U.S. at 403).

When compared with the description of other documents the government has properly withheld under the attorney-client privilege,[8] the twelve email conversations in the challenged documents here stand out because they do not involve anyone giving or receiving legal advice.[9] In *Coastal States*, the court ordered the release of legal memoranda that provided "neutral, objective analysis" of existing agency regulations in the context of specific factual questions from auditors in the field. *Id*. at 858. Because the memoranda were "practically binding" on auditors and their language resembled "question and answer guidelines in an agency manual," the court held that they were not "counseling" or advice subject to the privilege. *Id.*; *see also Safeway v. IRS*, No. 05-3182, 2006 U.S. Dist. LEXIS 81078, *28 (N.D. Cal. Oct. 24, 2006) (rejecting application of privilege to IRS counsel's "objective, neutral analysis" of application of tax regulations to plaintiff's tax returns). The information ICE and FBI have withheld reflect recitations of agency policy, rather than the give and take of legal counseling, even more closely than the *Coastal States* memoranda.

[8] Plaintiff does not challenge redactions under the Exemption 5 attorney-client privilege to FBI Bates Nos. 66-68, 72, 73, 74, 81, 110-113, 114-16, 117-118, 119-112, 144-45, 146-49. *See* Hardy Decl., Ex. I. Additionally, while Plaintiff does not challenge redactions to the email conversations at Bates Nos. 150-56 and 173-75 under the privilege, Plaintiff does challenge the unjustified withholding of two documents attached to the two email conversations at Bates Nos. 150-56 and 173-75. *See id.*

[9] FBI Bates Nos. 29-32, 33-34, 35-38, 40-41, 42-47, 48-54, 57-59, 65, 71, 76-77, 79-80, and document attached to Bates No. 58; DHS/ICE Vaughn Index Doc. 3.

Some emails actually describe the redacted sections as "standards," "guidance to personnel," and "procedures." *See respectively* FBI Bates Nos. 77-78 and 78-79, DHS/ICE Doc. 3. These terms and the unredacted language in some emails indicate that the communications are binding. *See, e.g.*, FBI Bates No. 71 ("FBI employees must comply with the section"). In other cases, the withheld material sounds like the "neutral, objective analysis" of existing policy released in *Coastal States*. *See* FBI Bates No. 58 (withheld attachment labeled "[redacted] policy examples" and described as "examples of how the [redacted] policy applies"). Because these documents do not contain legal advice, they are outside the scope of the attorney-client privilege and must be disclosed.

Moreover, because some of the FBI's emails formulate new guidelines for how the agency must interact with Internet service providers and users, rather than reflecting an attorney's confidential opinions, they are "working law" that cannot be withheld under Exemption 5. In *Tax Analysts v. IRS*, the court ordered the release of legal memoranda because their primary purpose was to create "a body of private law, applied routinely as the government's legal position in its dealings with taxpayers" and to ensure that agency staff applied regulations correctly and uniformly. 117 F.3d 607, 608-19 (D.C. Cir. 1997). The FBI has also improperly claimed the privilege to withhold agency "working law" in various emails that present new guidelines for obtaining user information from online service providers, using online services in investigations and using an undisclosed investigative technique, or communicate new guidance to ensure agents consistently applied a new investigative technique. FBI Bates Nos. 42-54, 76-77, 78-79.

Because the withheld emails do not reflect attorney-client confidences, and in some instances even act as guidelines governing how the government interacts with the public, the attorney-client privilege does not apply.

b. ICE Has Improperly Withheld Under the Attorney Work Product Privilege a Document That Was Not Prepared in Anticipation of Litigation and Does Not Contain Attorney Thoughts.

ICE has also improperly withheld an email conversation under Exemption 5, claiming the attorney work product privilege. DHS/ICE Doc. 3; Law Decl. ¶¶ 41-47. The privilege is applicable only when the document is (1) prepared in anticipation of litigation or for trial and (2) reveals

attorneys' thought processes. *Gerstein*, 2005 U.S. Dist. LEXIS 41276, at *47-48.

In *Gerstein*, the agency sought to withhold summaries of its use of delayed-notice warrants under the attorney work product doctrine, arguing that the documents reflected attorney work in individual cases. *Id*. at *48. The court rejected the argument, holding that the agency records were compiled for other purposes and were not prepared in anticipation of litigation. *Id*. The court also held that the summaries, which by their nature were high-level compilations, did not contain "insight into individual attorneys' thought processes." *Id*.

ICE has similarly failed to meet the privilege's threshold requirements. While the conversation between the agent and the attorney begins with the agent asking for guidance on a particular investigation, the attorney's high-level response is similar to the documents in *Gerstein*. Additionally, the attorney's response demonstrates that he did little more than provide an excerpt of ICE's general policy on the use of subpoenas to obtain information from Facebook. Because ICE has failed to show that the withheld record is protected by the work product privilege, it must be released.

c. Secret Service Has Improperly Withheld a Postdecisional Document Under the Exemption 5 Deliberative Process Privilege.

The Secret Service has improperly withheld one document under the Exemption 5 deliberative process privilege because it is postdecisional. Secret Service Doc. 11. The withheld memorandum reviews the effectiveness of a recently purchased system used to help the agency detect threats. Ulmer Decl. ¶¶ 54-55, 64-65. To qualify for the deliberative process privilege, an agency must show that the documents are predecisional, or prepared to assist an agency decision-maker in arriving at her decision, and deliberative, or used in agency decision-making such that disclosing them would discourage candid discussion within the agency. *Assembly of State of Cal. v. Dep't of Commerce*, 968 F.2d 916, 921 (9th Cir. 1992) (citing *Renegotiation Bd. v. Grumman Aircraft Eng'g Corp.*, 421 U.S. 168, 184 (1975)). Further, records that document a continuing process of agency self-examination cannot be withheld. *Maricopa Audubon Soc'y v. U.S. Forest Serv.*, 108 F.3d 1089, 1094 (9th Cir. 1997) (quoting *Coastal States*, 617 F.2d at 868).

In *Coastal States*, the agency sought to withhold under the deliberative process privilege an agency memo that periodically updated the standards the agency applied to a particular issue. 617 F.2d at 868. The court rejected the agency's argument, reasoning that the documents were auditing memos and that "[c]haracterizing these documents at 'predecisional' simply because they play into an ongoing audit process would be a serious warping of the meaning of the word." *Id*.

The nine-page Secret Service memorandum details the functionality and costs of a system used to identify threats. Further, the Secret Service has not pointed to a particular decision to which this memorandum contributed, as required under the privilege. *Coastal States*, 617 F.2d at 868. Much like the auditing document in *Coastal States*, the Secret Service memorandum reflects an ongoing assessment of an agency activity rather than deliberation about a particular decision. The memorandum must therefore be released.

3. Secret Service Has Improperly Withheld Documents under Exemption 4 That Do Not Pose Any Financial or Commercial Impairment Risk.

FOIA exempts from disclosure commercial or financial information that is "privileged or confidential." 5 U.S.C. § 552(b)(4). The Ninth Circuit defines Exemption 4's confidentiality protection as covering information that, if disclosed, would either (1) "impair the government's ability to obtain necessary information in the future," or (2) "cause substantial harm to the competitive position of the person from whom the information was obtained." *Frazee v. U.S. Forest Service*, 97 F.3d 367, 371 (9th Cir. 1996) (quoting and adopting the definition of Exemption 4's confidentiality withholding in *Nat'l Parks and Conservation Ass'n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974)).

The Secret Service has improperly withheld documents under Exemption 4 because it has failed to show that disclosing the documents will impair its future ability to receive similar information.[10] The Secret Service has withheld Documents 12-15 and 19-21, stating that they contain "information regarding the pricing, technical specifications, and performance capabilities of the company" with which it had contracts and claiming the agency will suffer impairment if the

[10] Plaintiff challenges the Secret Service's withholding under Exemption 4 of Documents 12-15 and 19-21.

documents are disclosed.[11] Def's Brf. 11; Ulmer Decl. ¶¶ 50-52; Ulmer Decl., Ex. G pp. 6-8, 10-12. However, disclosure of these documents will not impair the agency's ability to obtain such information in the future, because when contractors are required to submit financial information to an agency to secure a government contract, there is "presumably no danger that public disclosure will impair the ability of the Government to obtain this information in the future." *Nat'l Parks & Conservation Ass'n*, 498 F.2d at 770; *Raher v. Fed. Bureau of Prisons*, No. 09-526, 2011 WL 2014875, at *11 (D. Or. May 24, 2011).

In *National Parks*, the court held that Exemption 4 did not apply to audits of books of private concessioners employed by the National Park Service, holding that "[w]hether supplied pursuant to statute, regulation or some less formal mandate, however, it is clear that disclosure of this material to the Park Service is a mandatory condition of the concessioners' right to operate in national parks." *Id*. at 770. Following *National Parks*, the *Raher* court rejected the Bureau of Prisons' use of Exemption 4 to withhold records regarding the agency's contracts with companies that built prison facilities. *Raher*, 2011 WL 2014875 at *1. The court held that there was no impairment risk because the contractors were required to provide that information if they wanted to continue doing business with the agency. *Id*.

As in *Raher* and *National Parks*, contractors who wish to do business with the Secret Service must provide financial information before contracting with the agency. The Federal Acquisition Regulations System, which regulates government procurement, applies to contracts with the Secret Service. *See* 48 C.F.R. § 3002.101 (defining the Secret Service as a "component" of the Department of Homeland Security and subject to the regulations). The Federal Acquisition Regulations System requires contractors to disclose their costs as well as a description of their specifications and a statement of work. 48 C.F.R. §§ 15.204-2(b)-(c). Because the withheld information is a "mandatory condition" of doing business with the Secret Service, the Exemption 4

[11] The Secret Service does not argue that releasing the information would cause competitive harm to the private party who submitted the documents. Def's Brf. 11. The Secret Service has therefore conceded that no competitive harm exists and cannot rely upon it as a basis for the agency's withholdings.

claim must fail. The Secret Service bears no risk of losing access to "information regarding the pricing, technical specifications, and performance capabilities of the company" because contractors have a legal obligation to provide it.

B. Defendants' Conclusory Declarations and Vaughn Indices Do Not Adequately Support Their Exemption Claims.

In addition to the above, Defendants' declarations and Vaughn indices are also deficient in numerous instances, failing to satisfy their burden of providing specific, non-conclusory justifications for withholding exempt material.[12] The government may submit affidavits to show that it has properly withheld information, but "may not rely upon conclusory and generalized allegations of exemptions." *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir. 1995) (quoting *Church of Scientology v. Dep't of Army*, 611 F.2d 738, 742 (9th Cir. 1980) (internal quotation marks omitted). Courts in this District have routinely ordered the disclosure of materials when the government's declarations do not carry its burden. *See Feshbach,* 5 F. Supp. at 787; *Gerstein,* 2005 U.S. Dist. LEXIS 41276, at *41; *Safeway,* 2006 U.S. Dist. LEXIS 81078, at *28. Because Defendants in this case similarly rely on unsupported assertions to justify their exemption claims, the court should order the release all improperly withheld materials.

The inadequacy of Defendants' declarations is most evident in the FBI's withholding of several email attachments without any explanation. *See* Hardy Decl., Ex. I Bates Nos. 57-59, 78-80, 84-87, 126-29, 150-56, 218-23, 224-31, 232-39. More often, however, the explanations that Defendants provide simply fall short of sufficiently justifying their exemption claims. That insufficiency is also evident in many of the agencies' 7(E) claims. *Compare, e.g.,* DHS/ICE Document 3 (disclosure "could permit offenders to modify their conduct/conceal their activities in order to avoid detection, and thus, circumvent the law") *with Feshbach*, 5 F. Supp. 2d at 786 (rejecting as conclusory explanation that disclosure would "reveal Commission law enforcement procedures, techniques, and strategies, the disclosure of which could be used to circumvent federal securities laws"). Defendants' justifications for withholding information under Exemption 5

[12] Plaintiff challenges Defendants' failure to meet this burden with regard to all records listed in footnotes 4, 7, and 10 above.

are similarly inadequate. *Compare, e.g.*, Hardy Decl. pp. 84-85, Ex. I Bates Nos. 69-70 (describes deleted material as "request for legal input," but does not explain whether that "input" is legal advice); *id.* at p. 92, Bates Nos. 77-78 (asserting, without more, that "deletions comprise legal advice from OGC attorneys in response to questions from an FBI field office, i.e., the client") *with Ctr. for Biological Diversity v. OMB*, 625 F. Supp. 2d 885, 892 (N.D. Cal. 2009) (holding the government must do more than merely identify a document and invoke a privilege to meet its burden under Exemption 5).

C. ICE Failed to Adequately Search For Responsive Records.

ICE has not met its burden to conduct an adequate search, as it has failed to identify responsive documents similar to those that other agencies in this case have produced.

An agency bears the burden of proving that it conducted an adequate search. *Zemansky v. EPA*, 767 F.2d 569, 571 (9th Cir. 1985) (quoting *Weisberg v. DOJ,* 745 F.2d 1476, 1485 (D.C. Cir. 1984)). To meet its search obligations under the FOIA, an agency must produce evidence demonstrating that it conducted a "search reasonably calculated to uncover all relevant documents." *Id*. Courts apply a reasonableness standard when determining whether the agency's search for responsive documents was adequate, *Weisberg*, 745 F.2d at 1485, and view the facts in the light most favorable to the requestor. *Zemansky*, 767 F.2d at 571.

ICE has not conducted a search reasonably calculated to uncover all relevant documents because it failed to locate materials similar to those that other Defendants in this case found through their own searches. In response to EFF's FOIA request, other Defendants produced large amounts of records documenting their use of online social networks to investigate crimes. Notably, the FBI and the Secret Service produced third-party Law Enforcement Guides provided by social networking sites such as Facebook and MySpace. In his declaration, Deputy FOIA Officer Ryan Law describes how ICE tasked eight Special Agents—out of a total of 6,700 in the Office of Homeland Security Investigations, Lynch Decl. ¶ 33, Ex. 27—to search for responsive records. Law Decl. ¶ 18. It found 32 pages of responsive records. Law Decl. ¶ 37.

Even though ICE is the second-largest federal law enforcement agency in the country, Holzer Decl. ¶ 13—with a mission that includes combating cybercrime, Law Decl. ¶ 18—it did not locate *any* third-party law enforcement guides that its agents presumably use when investigating cybercrime. *See* Rich Lord, *Dozens sent to prison for trading child porn online*, Pittsburgh Post-Gazette (May 13, 2011) (discussing ICE's use and infiltration of social network Multiply.com to investigate a child pornography ring); Lynch Decl. ¶ 34, Ex. 28. Additionally, the discrepancy between what ICE and its co-Defendants in this case found through their searches demonstrates that ICE did not ensure that "the systems of records actually searched were those most likely to contain records responsive to the plaintiff's FOIA requests." *Lewis v. DOJ*, 733 F. Supp. 2d 97, 109 (D.D.C. 2010) (citing *Oglesby v. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990)). In short, ICE should have found records similar to those other agencies found because it has a similar enforcement mission and is larger than all other defendants except the FBI. The agency's failure to locate such records, or to explain exactly why such records would not be in its possession, indicates that ICE failed to conduct a search reasonably designed to locate responsive documents.

D. Defendants Have Failed to Meet Their Obligation of Segregating All Non-Exempt Material.

Finally, Defendants have also failed to meet their burden of showing that they have disclosed all reasonably segregable, non-exempt information from the hundreds of pages they have withheld in full or redacted almost in their entirety.[13] FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such a record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). The agency bears the burden of proving that it properly segregated. 5 U.S.C. § 552(a)(4)(b). All non-exempt portions of a document must be disclosed unless they are "inextricably entwined" with the exempt portions. *Willamette Indus. v. U.S.*, 689 F.2d 865, 867 (9th Cir. 1982) (citing *Mead Data Cent., Inc. v. Dep't of the Air Force*, 566 F.2d 242, 260-61 (D.C. Cir. 1977)). Courts must enter a segregability finding *sua sponte*. *Wiener v. FBI*, 943 F.2d 972, 988 (9th Cir. 1991).

[13] Plaintiff challenges Defendants' failure to meet this burden with regard to all records listed in footnotes 4, 7, and 10 above.

Defendants have failed to actually segregate and release all non-exempt information as required under the FOIA. Withholding large portions of material signals that agencies have likely failed to properly segregate. *See, e.g.*, *Bay Area Lawyers Alliance for Arms Control v. Dep't of State*, 818 F. Supp. 1291, 1300 (N.D. Cal. 1992) (reasoning, in the context of Exemption 5, that "it appears improbable that long documents are *entirely* 'analytical,' and do not contain any segregable *factual* material") (emphasis in original). Defendants' expansive withholdings in full under Exemptions 4, 5, and 7(E)[14] cannot be squared with the FOIA's segregability requirement. Nor can Defendants' overbroad redactions in partially released documents. *See, e.g.*, Holzer Decl., Ex 1 Doc. 3 (PowerPoint presentation redacted almost in its entirety). The Court should therefore order Defendants to disclose all reasonably segregable material.

Moreover, Defendants cannot meet their burden because their conclusory declarations fail to adequately justify their segregability decisions. Agencies must provide reasons for their segregability conclusions and tie them to specific facts about the withheld materials so that the plaintiff and court can review them. *NRDC v. Dep't of Defense*, 388 F. Supp. 2d 1086, 1096 (C.D. Cal. 2005) (citing *Mead Data*, 566 F.2d at 261). DHS's declaration fails to discuss segregability at all. Holzer Decl., Ex. 1. The other agencies provide only conclusory segregability explanations. *See, e.g.*, Ellis Decl. ¶ 39 (concluding without explanation that non-exempt material "is inextricably intertwined with non-exempt information and/or would be rendered meaningless if divorced from the exempt, responsive information"); Ulmer Decl. ¶ 67; Hardy Decl. ¶ 30; Law Decl. ¶ 52. The Court should therefore order the agencies to adequately justify their segregability determinations and release all segregable records.

V. CONCLUSION

For the foregoing reasons, Defendants' Motion for Summary Judgment should be denied, and Plaintiff's Cross Motion for Summary Judgment should be granted.

[14] S*ee, e.g.*, Secret Service Docs. 1-22 (agency's entire second production withheld in full); DOJ Items 3-4, 8-13 (150 pages withheld in full).

DATED: November 17, 2011

Respectfully submitted,

By: /s/ Jason M. Schultz

Jason M. Schultz
jschultz@law.berkeley.edu
Lila I. Bailey
SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
U.C. Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-1957
Facsimile: (510) 643-4625

Jennifer Lynch
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION